

Complete Weight Enumerators of Some Linear Codes

Shudi Yang and Zheng-An Yao

Abstract

Linear codes have been an interesting topic in both theory and practice for many years. In this paper, for an odd prime p , we determine the explicit complete weight enumerators of two classes of linear codes over \mathbb{F}_p and they may have applications in cryptography and secret sharing schemes. Moreover, some examples are included to illustrate our results.

Index Terms

Linear code, complete weight enumerator, quadratic form, Gauss sum.

I. INTRODUCTION

THROUGHOUT this paper, let p be an odd prime. Denote by \mathbb{F}_p a finite field with p elements. An $[n, \kappa, \delta]$ linear code C over \mathbb{F}_p is a κ -dimensional subspace of \mathbb{F}_p^n with minimum distance δ [1].

Let A_i denote the number of codewords with Hamming weight i in a linear code C of length n . The (ordinary) weight enumerator of C is defined by

$$A_0 + A_1z + A_2z^2 + \cdots + A_nz^n,$$

where $A_0 = 1$. The sequence $(A_0, A_1, A_2, \dots, A_n)$ is called the (ordinary) weight distribution of the code C .

The complete weight enumerator of a code C over \mathbb{F}_p enumerates the codewords according to the number of symbols of each kind contained in each codeword. Denote the field elements by $\mathbb{F}_p = \{w_0, w_1, \dots, w_{p-1}\}$, where $w_0 = 0$. Also let \mathbb{F}_p^* denote $\mathbb{F}_p \setminus \{0\}$. For a codeword $c = (c_0, c_1, \dots, c_{n-1}) \in \mathbb{F}_p^n$, let $w[c]$ be the complete weight enumerator of c defined as

$$w[c] = w_0^{k_0} w_1^{k_1} \cdots w_{p-1}^{k_{p-1}},$$

where k_j is the number of components of c equal to w_j , $\sum_{j=0}^{p-1} k_j = n$. The complete weight enumerator of the code C is then

$$\text{CWE}(C) = \sum_{c \in C} w[c].$$

The weight distribution of a linear code has attracted a lot of interest for many years and we refer the reader to [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13] and references therein for an overview of the related researches. It is not difficult to see that the complete weight enumerators are just the (ordinary) weight enumerators for binary linear codes. While for nonbinary linear codes, the weight enumerators can be obtained from their complete weight enumerators.

The information of the complete weight enumerator of a linear code is of vital use both in theories and in practical applications. For instance, Blake and Kith investigated the complete weight enumerator of Reed-Solomon codes and showed that they could be helpful in soft decision decoding [14], [15]. In [16], the study of the monomial and quadratic bent functions was related to the complete weight enumerators of linear codes. It was illustrated by Ding *et al.* [17], [18] that the complete weight enumerator can be applied to calculate the deception probabilities of certain authentication codes. In [19], [20], [21], the authors studied the complete weight enumerators of some constant composition codes and presented some families of optimal constant composition codes.

However, it is usually an extremely difficult problem to evaluate the complete weight enumerator of linear codes and there are few information on this topic in literature besides the above mentioned [14], [15], [19], [20], [21]. Kuzmin and Nechaev considered the generalized Kerdock code and related linear codes over Galois rings and determined their complete weight enumerators in [22] and [23]. Very recently, Li, Yue and Fu [24] obtained the complete weight enumerators of some cyclic codes by using Gauss sums. In this paper, we shall determine the complete weight enumerators of a class of linear codes over finite fields.

S.D. Yang is with the Department of Mathematics, Sun Yat-sen University, Guangzhou 510275 and School of Mathematical Sciences, Qufu Normal University, Shandong 273165, P.R.China.

Z.-A. Yao is with the Department of Mathematics, Sun Yat-sen University, Guangzhou 510275, P.R.China.

E-mail: yangshd3@mail2.sysu.edu.cn, mcsyao@mail.sysu.edu.cn

Manuscript received *****; revised *****.

Let $\bar{D} = \{d_1, d_2, \dots, d_n\} \subseteq \mathbb{F}_{p^m}$. Denote by Tr the trace function from \mathbb{F}_{p^m} to \mathbb{F}_p . A linear code associated with \bar{D} is defined by

$$C_{\bar{D}} = \{(\text{Tr}(ad_1), \text{Tr}(ad_2), \dots, \text{Tr}(ad_n)) : a \in \mathbb{F}_{p^m}\},$$

and \bar{D} is called the defining set of this code $C_{\bar{D}}$ (see [25], [26], [27] for details).

It should be noted that the authors in [25], [26] and [27] gave the definition of the code $C_{\bar{D}}$ and the defining set \bar{D} . The authors in [25] established binary linear codes $C_{\bar{D}}$ with three weights. In [26], Ding presented the general construction of the linear codes and determined their weights especially for three special codes. The authors in [27] presented the defining set $\bar{D} = \{x \in \mathbb{F}_{p^m}^* : \text{Tr}(x^2) = 0\}$ to construct a class of linear codes $C_{\bar{D}}$ with two and three nonzero weights and investigated their application in secret sharing.

In this paper, the defining set D of the code C_D is given by

$$D = \{x \in \mathbb{F}_{p^m}^* : \text{Tr}(x^{2d}) = 0\} = \{d_1, d_2, \dots, d_n\} \quad (1)$$

for an integer d coprime to $(p^m - 1)/2$, i.e., $\gcd(d, (p^m - 1)/2) = 1$. Let

$$C_D = \{(\text{Tr}(ad_1), \text{Tr}(ad_2), \dots, \text{Tr}(ad_n)) : a \in \mathbb{F}_{p^m}\}. \quad (2)$$

Note that $\gcd(d, (p^m - 1)/2) = 1$ leads to

$$\{x^{2d} : x \in \mathbb{F}_{p^m}^*\} = \{x^2 : x \in \mathbb{F}_{p^m}^*\},$$

which means that

$$\begin{aligned} D &= \{x \in \mathbb{F}_{p^m}^* : \text{Tr}(x^{2d}) = 0\} \\ &= \{x \in \mathbb{F}_{p^m}^* : \text{Tr}(x^2) = 0\} = \bar{D}. \end{aligned}$$

Therefore the codes C_D of (2) and $C_{\bar{D}}$ depicted in [27] are exactly the same code. Thus we only focus on the defining set

$$\bar{D} = \{x \in \mathbb{F}_{p^m}^* : \text{Tr}(x^2) = 0\} = \{d_1, d_2, \dots, d_n\}$$

in the sequel and we denote it by D for convenience.

More naturally, a generalization of the code C_D is given by

$$C_{D,b} = \{(\text{Tr}(ad_1) + b, \text{Tr}(ad_2) + b, \dots, \text{Tr}(ad_n) + b) : a \in \mathbb{F}_{p^m}, b \in \mathbb{F}_p\}. \quad (3)$$

We will study the complete weight enumerators of C_D and the generalized code $C_{D,b}$, and then their weight enumerators as well. As it turns out that, $C_{D,b}$ is a linear code with five and seven nonzero weights, while the code C_D is a linear code with two and three nonzero weights as was shown in [27]. This means that the two classes of linear codes may be of use in cryptography [28] and secret sharing schemes [29]. We should mention that the main idea of solving the complete weight enumerators of C_D and $C_{D,b}$ indeed comes from [26], [27] which were quite inspiring and very well-written and we will employ some results of [27] in the consequence sections.

The main results of this paper are given below.

Theorem 1. *Let D and C_D be defined as above.*

(A) *If $m \geq 3$ is odd, then the code C_D is a $[p^{m-1} - 1, m]$ linear code over \mathbb{F}_p with the complete weight enumerator*

$$\begin{aligned} \text{CWE}(C_D) &= w_0^{p^{m-1}-1} + (p^{m-1} - 1)w_0^{p^{m-2}-1} \prod_{\rho=1}^{p-1} w_\rho^{p^{m-2}} \\ &\quad + \frac{p-1}{2} \left(p^{m-1} + p^{\frac{m-1}{2}} \right) w_0^{p^{m-2}-1+(p-1)p^{\frac{m-3}{2}}} \prod_{\rho=1}^{p-1} w_\rho^{p^{m-2}-p^{\frac{m-3}{2}}} \\ &\quad + \frac{p-1}{2} \left(p^{m-1} - p^{\frac{m-1}{2}} \right) w_0^{p^{m-2}-1-(p-1)p^{\frac{m-3}{2}}} \prod_{\rho=1}^{p-1} w_\rho^{p^{m-2}+p^{\frac{m-3}{2}}} \end{aligned}$$

(B) *If $m \geq 2$ is even, then the code C_D over \mathbb{F}_p has parameters*

$$[p^{m-1} - 1 - (-1)^{\frac{m}{2}(\frac{p-1}{2})^2} (p-1)p^{\frac{m-2}{2}}, m]$$

and the complete weight enumerator

$$\begin{aligned}
& \text{CWE}(C_D) \\
&= w_0^{p^{m-1}-1-(-1)^{\frac{m}{2}(\frac{p-1}{2})^2}(p-1)p^{\frac{m-2}{2}}} + \\
& \quad \left(p^{m-1}-1-(-1)^{\frac{m}{2}(\frac{p-1}{2})^2}(p-1)p^{\frac{m-2}{2}} \right) w_0^{p^{m-2}-1-(-1)^{\frac{m}{2}(\frac{p-1}{2})^2}(p-1)p^{\frac{m-2}{2}}} \prod_{\rho=1}^{p-1} w_\rho^{p^{m-2}} + \\
& \quad (p-1) \left(p^{m-1} + (-1)^{\frac{m}{2}(\frac{p-1}{2})^2} p^{\frac{m-2}{2}} \right) w_0^{p^{m-2}-1} \prod_{\rho=1}^{p-1} w_\rho^{p^{m-2}-(-1)^{\frac{m}{2}(\frac{p-1}{2})^2} p^{\frac{m-2}{2}}}
\end{aligned}$$

Corollary 2. (See Theorems 1 and 2 of [27]) With notation as above.

(A) If $m \geq 3$ is odd, then C_D has the weight distribution given in Table I, where $A_i = 0$ for all other weights i not listed in the table.

TABLE I
THE WEIGHT DISTRIBUTION OF C_D FOR THE CASE OF ODD m

Weight i	Multiplicity A_i
0	1
$(p-1)(p^{m-2} - p^{\frac{m-3}{2}})$	$\frac{p-1}{2}(p^{m-1} + p^{\frac{m-1}{2}})$
$(p-1)p^{m-2}$	$p^{m-1} - 1$
$(p-1)(p^{m-2} + p^{\frac{m-3}{2}})$	$\frac{p-1}{2}(p^{m-1} - p^{\frac{m-1}{2}})$

(B) If $m \geq 2$ is even, then C_D has the weight distribution given in Table II, where $A_i = 0$ for all other weights i not listed in the table.

TABLE II
THE WEIGHT DISTRIBUTION OF C_D FOR THE CASE OF EVEN m

Weight i	Multiplicity A_i
0	1
$(p-1)p^{m-2}$	$p^{m-1} - (-1)^{\frac{m}{2}(\frac{p-1}{2})^2}(p-1)p^{\frac{m-2}{2}} - 1$
$(p-1)(p^{m-2} - (-1)^{\frac{m}{2}(\frac{p-1}{2})^2} p^{\frac{m-2}{2}})$	$(p-1)(p^{m-1} + (-1)^{\frac{m}{2}(\frac{p-1}{2})^2} p^{\frac{m-2}{2}})$

Example 3. (i) Let $(p, m) = (3, 5)$ and $d = 2$. Then the code C_D has parameters $[80, 5, 48]$ with complete weight enumerator

$$w_0^{80} + 90w_0^{32}w_1^{24}w_2^{24} + 80w_0^{26}w_1^{27}w_2^{27} + 72w_0^{20}w_1^{30}w_2^{30},$$

and weight enumerator

$$1 + 90z^{48} + 80z^{54} + 72z^{60}.$$

(ii) Let $(p, m) = (5, 4)$ and $d = 5$. Then the code C_D has parameters $[104, 4, 80]$ with complete weight enumerator

$$w_0^{104} + 520w_0^{24}w_1^{20}w_2^{20}w_3^{20}w_4^{20} + 104w_0^4w_1^{25}w_2^{25}w_3^{25}w_4^{25},$$

and weight enumerator

$$1 + 520z^{80} + 104z^{100}.$$

These results are consistent with numerical computation by Magma.

Theorem 4. Let D and $C_{D,b}$ be defined as above.

(A) If $m \geq 3$ is odd, then the code $C_{D,b}$ is a $[p^{m-1} - 1, m + 1]$ code over \mathbb{F}_p with the complete weight enumerator

$$\begin{aligned} \text{CWE}(C_{D,b}) &= \sum_{b=0}^{p-1} w_b^{p^{m-1}-1} + (p^{m-1} - 1) \sum_{b=0}^{p-1} w_b^{p^{m-2}-1} \prod_{\substack{\rho=0 \\ \rho \neq b}}^{p-1} w_\rho^{p^{m-2}} + \\ &\quad \frac{p-1}{2} \left(p^{m-1} + p^{\frac{m-1}{2}} \right) \sum_{b=0}^{p-1} w_b^{p^{m-2}-1+(p-1)p^{\frac{m-3}{2}}} \prod_{\substack{\rho=0 \\ \rho \neq b}}^{p-1} w_\rho^{p^{m-2}-p^{\frac{m-3}{2}}} + \\ &\quad \frac{p-1}{2} \left(p^{m-1} - p^{\frac{m-1}{2}} \right) \sum_{b=0}^{p-1} w_b^{p^{m-2}-1-(p-1)p^{\frac{m-3}{2}}} \prod_{\substack{\rho=0 \\ \rho \neq b}}^{p-1} w_\rho^{p^{m-2}+p^{\frac{m-3}{2}}}. \end{aligned}$$

(B) If $m \geq 2$ is even, then the code $C_{D,b}$ over \mathbb{F}_p has parameters

$$[p^{m-1} - 1 - (-1)^{\frac{m}{2}(\frac{p-1}{2})^2} (p-1)p^{\frac{m-2}{2}}, m + 1]$$

and the complete weight enumerator

$$\begin{aligned} \text{CWE}(C_{D,b}) &= \sum_{b=0}^{p-1} w_b^{p^{m-1}-1-(-1)^{\frac{m}{2}(\frac{p-1}{2})^2} (p-1)p^{\frac{m-2}{2}}} + \\ &\quad \left(p^{m-1}-1-(-1)^{\frac{m}{2}(\frac{p-1}{2})^2} (p-1)p^{\frac{m-2}{2}} \right) \sum_{b=0}^{p-1} w_b^{p^{m-2}-1-(-1)^{\frac{m}{2}(\frac{p-1}{2})^2} (p-1)p^{\frac{m-2}{2}}} \prod_{\substack{\rho=0 \\ \rho \neq b}}^{p-1} w_\rho^{p^{m-2}} + \\ &\quad (p-1) \left(p^{m-1} + (-1)^{\frac{m}{2}(\frac{p-1}{2})^2} p^{\frac{m-2}{2}} \right) \sum_{b=0}^{p-1} w_b^{p^{m-2}-1} \prod_{\substack{\rho=0 \\ \rho \neq b}}^{p-1} w_\rho^{p^{m-2}-(-1)^{\frac{m}{2}(\frac{p-1}{2})^2} p^{\frac{m-2}{2}}}. \end{aligned}$$

Corollary 5. With notation as above.

(A) If $m \geq 3$ is odd, then $C_{D,b}$ has the weight distribution given in Table III, where $A_i = 0$ for all other weights i not listed in the table.

TABLE III
THE WEIGHT DISTRIBUTION OF $C_{D,b}$ FOR THE CASE OF ODD m

Weight i	Multiplicity A_i
0	1
$p^{m-1} - 1$	$p - 1$
$(p-1)p^{m-2}$	$p^{m-1} - 1$
$(p-1)p^{m-2} - 1$	$(p-1)(p^{m-1} - 1)$
$(p-1)(p^{m-2} - p^{\frac{m-3}{2}})$	$\frac{p-1}{2}(p^{m-1} + p^{\frac{m-1}{2}})$
$(p-1)p^{m-2} + p^{\frac{m-3}{2}} - 1$	$\frac{(p-1)^2}{2}(p^{m-1} + p^{\frac{m-1}{2}})$
$(p-1)(p^{m-2} + p^{\frac{m-3}{2}})$	$\frac{p-1}{2}(p^{m-1} - p^{\frac{m-1}{2}})$
$(p-1)p^{m-2} - p^{\frac{m-3}{2}} - 1$	$\frac{(p-1)^2}{2}(p^{m-1} - p^{\frac{m-1}{2}})$

(B) If $m \geq 2$ is even, then $C_{D,b}$ has the weight distribution given in Table IV, where $A_i = 0$ for all other weights i not listed in the table.

Example 6. (i) Let $(p, m) = (3, 5)$ and $d = 2$. Then the code $C_{D,b}$ has parameters $[80, 6, 48]$ with complete weight enumerator

$$\begin{aligned} w_0^{80} &+ 90w_0^{32}w_1^{24}w_2^{24} + 72w_0^{30}w_1^{30}w_2^{20} + 72w_0^{30}w_1^{20}w_2^{30} + 80w_0^{27}w_1^{27}w_2^{26} \\ &+ 80w_0^{27}w_1^{26}w_2^{27} + 80w_0^{26}w_1^{27}w_2^{27} + 90w_0^{24}w_1^{32}w_2^{24} + 90w_0^{24}w_1^{24}w_2^{32} \\ &+ 72w_0^{20}w_1^{30}w_2^{30} + w_1^{80} + w_2^{80}, \end{aligned}$$

and weight enumerator

$$1 + 90z^{48} + 144z^{50} + 160z^{53} + 80z^{54} + 180z^{56} + 72z^{60} + 2z^{80}.$$

TABLE IV
THE WEIGHT DISTRIBUTION OF $C_{D,b}$ FOR THE CASE OF EVEN m

Weight i	Multiplicity A_i
0	1
$p^{m-1} - 1 - (-1)^{\frac{m}{2}(\frac{p-1}{2})^2} (p-1)p^{\frac{m-2}{2}}$	$p-1$
$(p-1)p^{m-2}$	$p^{m-1} - 1 - (-1)^{\frac{m}{2}(\frac{p-1}{2})^2} (p-1)p^{\frac{m-2}{2}}$
$(p-1)(p^{m-2} - (-1)^{\frac{m}{2}(\frac{p-1}{2})^2} p^{\frac{m-2}{2}}) - 1$	$(p-1)(p^{m-1} - 1 - (-1)^{\frac{m}{2}(\frac{p-1}{2})^2} (p-1)p^{\frac{m-2}{2}})$
$(p-1)(p^{m-2} - (-1)^{\frac{m}{2}(\frac{p-1}{2})^2} p^{\frac{m-2}{2}})$	$(p-1)(p^{m-1} + (-1)^{\frac{m}{2}(\frac{p-1}{2})^2} p^{\frac{m-2}{2}})$
$(p-1)p^{m-2} - (p-2)(-1)^{\frac{m}{2}(\frac{p-1}{2})^2} p^{\frac{m-2}{2}} - 1$	$(p-1)^2(p^{m-1} + (-1)^{\frac{m}{2}(\frac{p-1}{2})^2} p^{\frac{m-2}{2}})$

(ii) Let $(p, m) = (3, 4)$ and $d = 3$. Then the code $C_{D,b}$ has parameters $[20, 5, 11]$ with complete weight enumerator

$$\begin{aligned} w_0^{20} &+ 20w_0^9w_1^9w_2^2 + 20w_0^9w_1^2w_2^9 + 60w_0^8w_1^6w_2^6 + 60w_0^6w_1^8w_2^6 \\ &+ 60w_0^6w_1^6w_2^8 + 20w_0^2w_1^9w_2^9 + w_1^{20} + w_2^{20}, \end{aligned}$$

and weight enumerator

$$1 + 40z^{11} + 60z^{12} + 120z^{14} + 20z^{18} + 2z^{20}.$$

We can check these results by using Magma.

The remainder of this paper is organized as follows. In Section II, we recall some definitions and results on quadratic forms and Gauss sums over finite fields. Section III is devoted to the proofs of Theorems 1 and 4, respectively. Section IV concludes this paper and makes some remarks on this topic.

II. MATHEMATICAL FOUNDATIONS

We start with quadratic forms over finite fields. Let q be a power of p and t be a positive integer. By identifying the finite field \mathbb{F}_{q^t} with a t -dimensional vector space \mathbb{F}_q^t over \mathbb{F}_q , a function $f(x)$ from \mathbb{F}_{q^t} to \mathbb{F}_q can be regarded as a t -variable polynomial over \mathbb{F}_q . The function $f(x)$ is called a quadratic form if it can be written as a homogeneous polynomial of degree two on \mathbb{F}_q^t as follows:

$$f(x_1, x_2, \dots, x_t) = \sum_{1 \leq i \leq j \leq t} a_{ij} x_i x_j, \quad a_{ij} \in \mathbb{F}_q.$$

Here we fix a basis of \mathbb{F}_{q^t} over \mathbb{F}_q and identify each $x \in \mathbb{F}_{q^t}$ with a vector $(x_1, x_2, \dots, x_t) \in \mathbb{F}_q^t$. The rank of the quadratic form $f(x)$, $\text{rank}(f)$, is defined as the codimension of the \mathbb{F}_q -vector space

$$W = \{x \in \mathbb{F}_{q^t} \mid f(x+z) - f(x) - f(z) = 0, \text{ for all } z \in \mathbb{F}_{q^t}\}.$$

Then $|W| = q^{t-\text{rank}(f)}$.

For a quadratic form $f(x)$ with t variables over \mathbb{F}_q , there exists a symmetric matrix A of order t over \mathbb{F}_q such that $f(x) = XAX'$, where $X = (x_1, x_2, \dots, x_t) \in \mathbb{F}_q^t$ and X' denotes the transpose of X . It is known that there exists a nonsingular matrix B over \mathbb{F}_q such that BAB' is a diagonal matrix. Making a nonsingular linear substitution $X = YB$ with $Y = (y_1, y_2, \dots, y_t) \in \mathbb{F}_q^t$, we have

$$f(x) = Y(BAB')Y' = \sum_{i=1}^r a_i y_i^2, \quad a_i \in \mathbb{F}_q^*,$$

where r is the rank of $f(x)$. The determinant $\det(f)$ of $f(x)$ is defined to be the determinant of A , and $f(x)$ is said to be nondegenerate if $\det(f) \neq 0$.

Lemma 7. (See Theorems 6.26 and 6.27 of [30]) Let f be a nondegenerate quadratic form over \mathbb{F}_q , $q = p^t$ for odd prime p , in l variables. Define a function $v(\cdot)$ over \mathbb{F}_q by $v(0) = q - 1$ and $v(\rho) = -1$ for $\rho \in \mathbb{F}_q^*$. Then for $b \in \mathbb{F}_q$ the number of solutions of the equation $f(x_1, \dots, x_l) = b$ is

$$\begin{cases} q^{l-1} + v(b)q^{\frac{l-2}{2}}\eta_t\left((-1)^{\frac{l}{2}}\det(f)\right), & \text{if } l \text{ is even,} \\ q^{l-1} + q^{\frac{l-1}{2}}\eta_t\left((-1)^{\frac{l-1}{2}}b\det(f)\right), & \text{if } l \text{ is odd,} \end{cases}$$

where η_t is the quadratic character of \mathbb{F}_q defined by

$$\eta_t(x) = \begin{cases} 1, & \text{if } x \text{ is a square in } \mathbb{F}_{p^t}^*, \\ -1, & \text{if } x \text{ is a nonsquare in } \mathbb{F}_{p^t}^*, \\ 0, & \text{if } x = 0. \end{cases}$$

The canonical additive character of \mathbb{F}_{p^m} , denoted χ , is given by

$$\chi(x) = \zeta_p^{\text{Tr}(x)}$$

for all $x \in \mathbb{F}_{p^m}$, where $\zeta_p = e^{2\pi\sqrt{-1}/p}$ and Tr is a trace function from \mathbb{F}_{p^m} to \mathbb{F}_p defined by

$$\text{Tr}(x) = \sum_{i=0}^{m-1} x^{p^i}, \quad x \in \mathbb{F}_{p^m}.$$

In what follows, we abbreviate η_m as η for simplicity. The quadratic Gauss sum $G(\eta, \chi)$ over \mathbb{F}_{p^m} is defined by

$$G(\eta, \chi) = \sum_{x \in \mathbb{F}_{p^m}^*} \eta(x) \chi(x) = \sum_{x \in \mathbb{F}_{p^m}} \eta(x) \chi(x),$$

and the quadratic Gauss sum $G(\bar{\eta}, \bar{\chi})$ over \mathbb{F}_p is defined by

$$G(\bar{\eta}, \bar{\chi}) = \sum_{x \in \mathbb{F}_p^*} \bar{\eta}(x) \bar{\chi}(x) = \sum_{x \in \mathbb{F}_p} \bar{\eta}(x) \bar{\chi}(x),$$

where $\bar{\eta}$ and $\bar{\chi}$ are the quadratic and canonical additive characters of \mathbb{F}_p , respectively.

The lemmas introduced below will play an important role in the sequel.

Lemma 8. (See Theorems 5.15 [30]) *With the symbols and notation above, we have*

$$G(\eta, \chi) = (-1)^{m-1} (\sqrt{-1})^{\frac{(p-1)^2}{4} m} p^{\frac{m}{2}}, \quad (4)$$

and

$$G(\bar{\eta}, \bar{\chi}) = (\sqrt{-1})^{\frac{(p-1)^2}{4}} p^{\frac{1}{2}}. \quad (5)$$

Lemma 9. (See Theorem 5.33 of [30]) *With the symbols and notation above. Let $f(x) = a_2 x^2 + a_1 x + a_0 \in \mathbb{F}_{p^m}[x]$ with $a_2 \neq 0$. Then*

$$\sum_{x \in \mathbb{F}_{p^m}} \chi(f(x)) = \chi(a_0 - a_1^2(4a_2)^{-1}) \eta(a_2) G(\eta, \chi).$$

Lemma 10. (See Lemma 7 of [27]) *If $m \geq 2$ is even, then $\eta(y) = 1$ for each $y \in \mathbb{F}_p^*$. If m is odd, then $\eta(y) = \bar{\eta}(y)$ for each $y \in \mathbb{F}_p$.*

Lemma 11. (See Lemma 8 of [27]) *We have the following equality:*

$$\sum_{y \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{y \text{Tr}(x^2)} = \begin{cases} 0 & \text{if } m \text{ odd,} \\ (-1)^{m-1} (-1)^{\frac{m}{2} (\frac{p-1}{2})^2} (p-1) p^{\frac{m}{2}} & \text{if } m \text{ even.} \end{cases}$$

Lemma 12. (See Lemma 9 of [27]) *Let $n_0 = \#\{x \in \mathbb{F}_{p^m} : \text{Tr}(x^2) = 0\}$. Then*

$$n_0 = \begin{cases} p^{m-1} & \text{if } m \text{ odd,} \\ p^{m-1} - (-1)^{\frac{m}{2} (\frac{p-1}{2})^2} (p-1) p^{\frac{m-2}{2}} & \text{if } m \text{ even.} \end{cases}$$

III. THE PROOFS OF THE MAIN RESULTS

Our task of this section is to prove Theorems 1 and 4 depicted in Section I, while Corollary 5 follows immediately from Theorem 4. In the following, a series of auxiliary results are described and proved for this purpose.

Lemma 13. *Let $a \in \mathbb{F}_{p^m}^*$ and $\rho \in \mathbb{F}_p$. Then, for $m \geq 3$ being odd, we have*

$$\begin{aligned} & \sum_{y \in \mathbb{F}_p^*} \sum_{z \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\text{Tr}(yx^2 + azx) - z\rho} \\ &= \begin{cases} 0 & \text{if } \text{Tr}(a^2) = 0 \text{ and } \rho = 0, \\ 0 & \text{if } \text{Tr}(a^2) = 0 \text{ and } \rho \neq 0, \\ (-1)^{\frac{m-1}{2} \frac{p-1}{2}} (p-1) p^{\frac{m+1}{2}} \bar{\eta}(\text{Tr}(a^2)) & \text{if } \text{Tr}(a^2) \neq 0 \text{ and } \rho = 0, \\ -(-1)^{\frac{m-1}{2} \frac{p-1}{2}} p^{\frac{m+1}{2}} \bar{\eta}(\text{Tr}(a^2)) & \text{if } \text{Tr}(a^2) \neq 0 \text{ and } \rho \neq 0, \end{cases} \end{aligned}$$

and for $m \geq 2$ being even, we have

$$\begin{aligned} & \sum_{y \in \mathbb{F}_p^*} \sum_{z \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\text{Tr}(yx^2+azx)-z\rho} \\ &= \begin{cases} -(-1)^{\frac{m}{2}(\frac{p-1}{2})^2} (p-1)^2 p^{\frac{m}{2}} & \text{if } \text{Tr}(a^2) = 0 \text{ and } \rho = 0, \\ (-1)^{\frac{m}{2}(\frac{p-1}{2})^2} (p-1) p^{\frac{m}{2}} & \text{if } \text{Tr}(a^2) = 0 \text{ and } \rho \neq 0, \\ (-1)^{\frac{m}{2}(\frac{p-1}{2})^2} (p-1) p^{\frac{m}{2}} & \text{if } \text{Tr}(a^2) \neq 0 \text{ and } \rho = 0, \\ -(-1)^{\frac{m}{2}(\frac{p-1}{2})^2} p^{\frac{m}{2}} & \text{if } \text{Tr}(a^2) \neq 0 \text{ and } \rho \neq 0. \end{cases} \end{aligned}$$

Proof: It follows from Lemmas 9 and 10 that

$$\begin{aligned} & \sum_{y \in \mathbb{F}_p^*} \sum_{z \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\text{Tr}(yx^2+azx)-z\rho} \\ &= \sum_{z \in \mathbb{F}_p^*} \zeta_p^{-z\rho} \sum_{y \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\text{Tr}(yx^2+azx)} \\ &= \sum_{z \in \mathbb{F}_p^*} \zeta_p^{-z\rho} \sum_{y \in \mathbb{F}_p^*} \chi\left(-\frac{a^2 z^2}{4y}\right) \eta(y) G(\eta, \chi) \\ &= G(\eta, \chi) \sum_{z \in \mathbb{F}_p^*} \zeta_p^{-z\rho} \sum_{y_1 \in \mathbb{F}_p^*} \chi(-a^2 z^2 y_1) \eta\left(\frac{1}{4y_1}\right) \\ &= G(\eta, \chi) \sum_{z \in \mathbb{F}_p^*} \zeta_p^{-z\rho} \sum_{y \in \mathbb{F}_p^*} \chi(-a^2 z^2 y) \eta(y) \\ &= G(\eta, \chi) \sum_{z \in \mathbb{F}_p^*} \zeta_p^{-z\rho} \sum_{y \in \mathbb{F}_p^*} \zeta_p^{-z^2 \text{Tr}(a^2)y} \eta(y) \\ &= \begin{cases} G(\eta, \chi) \sum_{z \in \mathbb{F}_p^*} \zeta_p^{-z\rho} \sum_{y \in \mathbb{F}_p^*} \eta(y) & \text{if } \text{Tr}(a^2) = 0, \\ G(\eta, \chi) \sum_{z \in \mathbb{F}_p^*} \zeta_p^{-z\rho} \sum_{y \in \mathbb{F}_p^*} \zeta_p^{-z^2 \text{Tr}(a^2)y} \eta(-z^2 \text{Tr}(a^2)y) \eta(-\text{Tr}(a^2)) & \text{if } \text{Tr}(a^2) \neq 0. \end{cases} \end{aligned}$$

For the case of m being odd, by Lemma 10, we have

$$\begin{aligned} & \sum_{y \in \mathbb{F}_p^*} \sum_{z \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\text{Tr}(yx^2+azx)-z\rho} \\ &= \begin{cases} G(\eta, \chi) \sum_{z \in \mathbb{F}_p^*} \zeta_p^{-z\rho} \sum_{y \in \mathbb{F}_p^*} \bar{\eta}(y) & \text{if } \text{Tr}(a^2) = 0 \\ G(\eta, \chi) \sum_{z \in \mathbb{F}_p^*} \zeta_p^{-z\rho} \sum_{y \in \mathbb{F}_p^*} \zeta_p^{-z^2 \text{Tr}(a^2)y} \bar{\eta}(-z^2 \text{Tr}(a^2)y) \bar{\eta}(-\text{Tr}(a^2)) & \text{if } \text{Tr}(a^2) \neq 0 \end{cases} \\ &= \begin{cases} 0 & \text{if } \text{Tr}(a^2) = 0 \\ G(\eta, \chi) \sum_{z \in \mathbb{F}_p^*} \zeta_p^{-z\rho} G(\bar{\eta}, \bar{\chi}) \bar{\eta}(-\text{Tr}(a^2)) & \text{if } \text{Tr}(a^2) \neq 0 \end{cases} \\ &= \begin{cases} 0 & \text{if } \text{Tr}(a^2) = 0 \text{ and } \rho = 0, \\ 0 & \text{if } \text{Tr}(a^2) = 0 \text{ and } \rho \neq 0, \\ (p-1)G(\eta, \chi)G(\bar{\eta}, \bar{\chi})\bar{\eta}(-\text{Tr}(a^2)) & \text{if } \text{Tr}(a^2) \neq 0 \text{ and } \rho = 0, \\ -G(\eta, \chi)G(\bar{\eta}, \bar{\chi})\bar{\eta}(-\text{Tr}(a^2)) & \text{if } \text{Tr}(a^2) \neq 0 \text{ and } \rho \neq 0. \end{cases} \end{aligned}$$

The desired conclusions then follow from Lemma 8 and the fact that

$$(-1)^{\frac{p-1}{2} + \frac{m+1}{2}(\frac{p-1}{2})^2} = (-1)^{\frac{m-1}{2} \frac{p-1}{2}}.$$

Similarly, for the case of m being even, we can deduce that

$$\begin{aligned} & \sum_{y \in \mathbb{F}_p^*} \sum_{z \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\text{Tr}(yx^2+azx)-z\rho} \\ &= \begin{cases} (p-1)G(\eta, \chi) \sum_{z \in \mathbb{F}_p^*} \zeta_p^{-z\rho} & \text{if } \text{Tr}(a^2) = 0 \\ -G(\eta, \chi) \sum_{z \in \mathbb{F}_p^*} \zeta_p^{-z\rho} & \text{if } \text{Tr}(a^2) \neq 0 \end{cases} \\ &= \begin{cases} (p-1)^2 G(\eta, \chi) & \text{if } \text{Tr}(a^2) = 0 \text{ and } \rho = 0, \\ -(p-1)G(\eta, \chi) & \text{if } \text{Tr}(a^2) = 0 \text{ and } \rho \neq 0, \\ -(p-1)G(\eta, \chi) & \text{if } \text{Tr}(a^2) \neq 0 \text{ and } \rho = 0, \\ G(\eta, \chi) & \text{if } \text{Tr}(a^2) \neq 0 \text{ and } \rho \neq 0. \end{cases} \end{aligned}$$

From Lemma 8 again, we obtain the desired conclusions. ■

Lemma 14. For any $a \in \mathbb{F}_{p^m}^*$ and any $\rho \in \mathbb{F}_p$, let

$$N_a(\rho) = \#\{x \in \mathbb{F}_{p^m} : \text{Tr}(x^2) = 0 \text{ and } \text{Tr}(ax) = \rho\}.$$

Then, for $m \geq 3$ being odd, we have

$$N_a(\rho) = \begin{cases} p^{m-2} & \text{if } \text{Tr}(a^2) = 0 \text{ and } \rho = 0, \\ p^{m-2} & \text{if } \text{Tr}(a^2) = 0 \text{ and } \rho \neq 0, \\ p^{m-2} + (-1)^{\frac{m-1}{2}} \frac{p-1}{2} p^{\frac{m-3}{2}} \bar{\eta}(\text{Tr}(a^2)) & \text{if } \text{Tr}(a^2) \neq 0 \text{ and } \rho = 0, \\ p^{m-2} - (-1)^{\frac{m-1}{2}} \frac{p-1}{2} p^{\frac{m-3}{2}} \bar{\eta}(\text{Tr}(a^2)) & \text{if } \text{Tr}(a^2) \neq 0 \text{ and } \rho \neq 0, \end{cases}$$

and for $m \geq 2$ being even, we have

$$N_a(\rho) = \begin{cases} p^{m-2} - (-1)^{\frac{m}{2}} \left(\frac{p-1}{2}\right)^2 (p-1) p^{\frac{m-2}{2}} & \text{if } \text{Tr}(a^2) = 0 \text{ and } \rho = 0, \\ p^{m-2} & \text{if } \text{Tr}(a^2) = 0 \text{ and } \rho \neq 0, \\ p^{m-2} & \text{if } \text{Tr}(a^2) \neq 0 \text{ and } \rho = 0, \\ p^{m-2} - (-1)^{\frac{m}{2}} \left(\frac{p-1}{2}\right)^2 p^{\frac{m-2}{2}} & \text{if } \text{Tr}(a^2) \neq 0 \text{ and } \rho \neq 0. \end{cases}$$

Proof: For any $a \in \mathbb{F}_{p^m}^*$ and any $\rho \in \mathbb{F}_p$, we have

$$\begin{aligned} N_a(\rho) &= p^{-2} \sum_{x \in \mathbb{F}_{p^m}} \left(\sum_{y \in \mathbb{F}_p} \zeta_p^{y \text{Tr}(x^2)} \right) \left(\sum_{z \in \mathbb{F}_p} \zeta_p^{z(\text{Tr}(ax) - \rho)} \right) \\ &= p^{-2} \sum_{z \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{z(\text{Tr}(ax) - \rho)} + p^{-2} \sum_{y \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{y \text{Tr}(x^2)} + \\ &\quad p^{-2} \sum_{y \in \mathbb{F}_p^*} \sum_{z \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{\text{Tr}(yx^2 + axz) - z\rho} + p^{m-2}. \end{aligned}$$

Note that

$$\sum_{z \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{z(\text{Tr}(ax) - \rho)} = \sum_{z \in \mathbb{F}_p^*} \zeta_p^{-z\rho} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{z \text{Tr}(ax)} = 0$$

since

$$\sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{z \text{Tr}(ax)} = \begin{cases} p^m, & \text{if } z = 0, \\ 0, & \text{if } z \in \mathbb{F}_p^*. \end{cases}$$

The desired conclusions then follow from Lemma 11 and 13. ■

Lemma 15. Suppose that $m \geq 3$ is odd. Let $t_i = \#\{x \in \mathbb{F}_{p^m}^* : \bar{\eta}(\text{Tr}(x^2)) = i\}$ with $i \in \{0, 1, -1\}$. Then

$$\begin{cases} t_0 &= p^{m-1} - 1, \\ t_1 &= \frac{p-1}{2} \left(p^{m-1} + (-1)^{\frac{m-1}{2}} \frac{p-1}{2} p^{\frac{m-1}{2}} \right), \\ t_{-1} &= \frac{p-1}{2} \left(p^{m-1} - (-1)^{\frac{m-1}{2}} \frac{p-1}{2} p^{\frac{m-1}{2}} \right). \end{cases}$$

Proof: The case $i = 0$ follows from Lemma 12.

We only give the proof of the case $i = 1$ since the other case $i = -1$ is similar.

Note that $\bar{\eta}(\text{Tr}(x^2)) = 1$ if and only if $\text{Tr}(x^2) = \beta$, where β is a quadratic residue over \mathbb{F}_p .

For each $x \in \mathbb{F}_{p^m}^*$, we can verify that $\text{Tr}(x^2)$ is a quadratic form over \mathbb{F}_p with rank m . It follows at once that $\text{Tr}(x^2) = \beta$ can be transformed into the form

$$\sum_{i=1}^m x_i^2 = \beta, \tag{6}$$

under an orthonormal basis $\{\alpha_1, \alpha_2, \dots, \alpha_m\}$ of \mathbb{F}_{p^m} over \mathbb{F}_p and $x = \sum_{i=1}^m x_i \alpha_i$ with $x_i \in \mathbb{F}_p$.

Since \mathbb{F}_p contains $(p-1)/2$ quadratic residues, the desired conclusion then follows from Equation (6) and Lemma 7. ■

A. The proof of Theorem 1

Recall that

$$C_D = \{(\text{Tr}(ad_1), \text{Tr}(ad_2), \dots, \text{Tr}(ad_n)) : a \in \mathbb{F}_{p^m}\},$$

where $D = \{x \in \mathbb{F}_{p^m}^* : \text{Tr}(x^2) = 0\}$.

By Lemma 12, the length n of C_D is given by

$$n = n_0 - 1 = \begin{cases} p^{m-1} - 1 & \text{if } m \text{ odd,} \\ p^{m-1} - 1 - (-1)^{\frac{m}{2}(\frac{p-1}{2})^2} (p-1)p^{\frac{m-2}{2}} & \text{if } m \text{ even.} \end{cases} \quad (7)$$

Clearly $a = 0$ gives the zero codeword and the contribution to the complete weight enumerator is w_0^n .

Assume that $a \in \mathbb{F}_{p^m}^*$ for the rest of the proof. To determine the complete weight enumerator of each codeword

$$(\text{Tr}(ad_1), \text{Tr}(ad_2), \dots, \text{Tr}(ad_n)),$$

we need to consider the number of solutions $x \in \mathbb{F}_{p^m}^*$ satisfying $\text{Tr}(x^2) = 0$ and $\text{Tr}(ax) = \rho$ with $\rho \in \mathbb{F}_p$, i.e.,

$$n_a(\rho) = \#\{x \in \mathbb{F}_{p^m}^* : \text{Tr}(x^2) = 0 \text{ and } \text{Tr}(ax) = \rho\}.$$

It is clearly that

$$n_a(\rho) = \begin{cases} N_a(\rho) - 1, & \text{if } \rho = 0, \\ N_a(\rho), & \text{if } \rho \neq 0. \end{cases}$$

When $m \geq 3$ is odd, it follows from Lemma 14 that

$$n_a(\rho) = \begin{cases} p^{m-2} - 1 & \text{if } \text{Tr}(a^2) = 0 \text{ and } \rho = 0, \\ p^{m-2} & \text{if } \text{Tr}(a^2) = 0 \text{ and } \rho \neq 0, \\ p^{m-2} - 1 + (-1)^{\frac{m-1}{2} \frac{p-1}{2}} (p-1)p^{\frac{m-3}{2}} \bar{\eta}(\text{Tr}(a^2)) & \text{if } \text{Tr}(a^2) \neq 0 \text{ and } \rho = 0, \\ p^{m-2} - (-1)^{\frac{m-1}{2} \frac{p-1}{2}} p^{\frac{m-3}{2}} \bar{\eta}(\text{Tr}(a^2)) & \text{if } \text{Tr}(a^2) \neq 0 \text{ and } \rho \neq 0, \end{cases}$$

When $m \geq 2$ is even, Lemma 14 shows that

$$n_a(\rho) = \begin{cases} p^{m-2} - 1 - (-1)^{\frac{m}{2}(\frac{p-1}{2})^2} (p-1)p^{\frac{m-2}{2}} & \text{if } \text{Tr}(a^2) = 0 \text{ and } \rho = 0 \\ p^{m-2} & \text{if } \text{Tr}(a^2) = 0 \text{ and } \rho \neq 0 \\ p^{m-2} - 1 & \text{if } \text{Tr}(a^2) \neq 0 \text{ and } \rho = 0 \\ p^{m-2} - (-1)^{\frac{m}{2}(\frac{p-1}{2})^2} p^{\frac{m-2}{2}} & \text{if } \text{Tr}(a^2) \neq 0 \text{ and } \rho \neq 0 \end{cases}$$

The desired conclusions of Theorem 1 then follow from Lemmas 12 and 15.

B. The proof of Theorem 4

Recall that

$$C_{D,b} = \{(\text{Tr}(ad_1) + b, \text{Tr}(ad_2) + b, \dots, \text{Tr}(ad_n) + b) : a \in \mathbb{F}_{p^m}, b \in \mathbb{F}_p\},$$

where $D = \{x \in \mathbb{F}_{p^m}^* : \text{Tr}(x^2) = 0\}$. Obviously, $C_{D,b}$ has the same length n of (7) as that of C_D .

The complete weight enumerator of $C_{D,b}$ can be explicitly determined by distinguishing the following cases.

Case 1: $a = 0$ and $b \in \mathbb{F}_p$.

It can be seen that the corresponding codeword of length n contains b in each coordinate position, which contributes to the complete weight enumerator w_b^n for each $b \in \mathbb{F}_p$. Then the total contribution of such terms to the complete weight enumerator is

$$\sum_{b=0}^{p-1} w_b^n.$$

Case 2: $a \neq 0$ and $b \in \mathbb{F}_p$.

In this case, we consider

$$n_{a,b}(\rho + b) = \#\{x \in \mathbb{F}_{p^m}^* : \text{Tr}(x^2) = 0 \text{ and } \text{Tr}(ax) + b = \rho + b\},$$

which leads to

$$n_{a,b}(\rho + b) = n_a(\rho).$$

For a fixed $a \in \mathbb{F}_{p^m}^*$, let $(\text{Tr}(ad_1), \text{Tr}(ad_2), \dots, \text{Tr}(ad_n))$ be a nonzero codeword in C_D with complete weight enumerator

$$w_0^{n_a(0)} w_1^{n_a(1)} \dots w_{p-1}^{n_a(p-1)}.$$

By the definition of $C_{D,b}$, for a fixed $b \in \mathbb{F}_p$, the corresponding nonzero codeword in $C_{D,b}$ is

$$(\text{Tr}(ad_1) + b, \text{Tr}(ad_2) + b, \dots, \text{Tr}(ad_n) + b),$$

and its contribution to the complete weight enumerator is

$$w_b^{n_a(0)} w_{1+b}^{n_a(1)} \dots w_{p-1+b}^{n_a(p-1)}.$$

As b runs through \mathbb{F}_p , this means that the contributions of such terms to the complete weight enumerator are of the form

$$\sum_{b=0}^{p-1} w_b^{n_a(0)} w_{1+b}^{n_a(1)} \dots w_{p-1+b}^{n_a(p-1)}.$$

Therefore, the desired conclusions follow from Theorem 1.

IV. CONCLUDING REMARKS

In this paper, we proposed the complete weight enumerators of two classes of the linear codes C_D and $C_{D,b}$ with defining set D for the case of $\gcd(d, (p^m - 1)/2) = 1$. The ideas of the proofs of Theorems 1 and 4 came from [26], [27].

It should be pointed out that the weight enumerator of C_D was determined in [27]. And we described the weight enumerator of $C_{D,b}$ which follows directly from its complete weight enumerator. Some examples were given to confirm our conclusions.

V. ACKNOWLEDGEMENTS

The work of Zheng-An Yao is partially supported by the NSFC (Grant No.11271381), the NSFC (Grant No.11431015) and China 973 Program (Grant No. 2011CB808000). This work is also partially supported by the NSFC (Grant No.61472457) and Guangdong Natural Science Foundation (Grant No. 2014A030313161).

REFERENCES

- [1] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*. North-Holland Publishing, Amsterdam, 1977, vol. 16.
- [2] D. Zheng, X. Wang, L. Yu, and H. Liu, "The weight enumerators of several classes of p -ary cyclic codes," *Discrete Mathematics*, vol. 338, no. 7, pp. 1264–1276, 2015.
- [3] C. Ding, Y. Liu, C. Ma, and L. Zeng, "The weight distributions of the duals of cyclic codes with two zeros," *IEEE Transactions on Information Theory*, vol. 57, no. 12, pp. 8000–8006, 2011.
- [4] C. Ding and J. Yang, "Hamming weights in irreducible cyclic codes," *Discrete Mathematics*, vol. 313, no. 4, pp. 434–446, 2013.
- [5] H. Q. Dinh, C. Li, and Q. Yue, "Recent progress on weight distributions of cyclic codes over finite fields," *Journal of Algebra Combinatorics Discrete Structures and Applications*, vol. 2, no. 1, pp. 39–63, 2015.
- [6] K. Feng and J. Luo, "Weight distribution of some reducible cyclic codes," *Finite Fields and Their Applications*, vol. 14, no. 2, pp. 390–409, 2008.
- [7] C. Li and Q. Yue, "Weight distributions of two classes of cyclic codes with respect to two distinct order elements," *IEEE Transactions on Information Theory*, vol. 60, no. 1, pp. 296–303, Jan 2014.
- [8] J. Luo and K. Feng, "On the weight distributions of two classes of cyclic codes," *IEEE Transactions on Information Theory*, vol. 54, no. 12, pp. 5332–5344, Dec 2008.
- [9] A. Sharma and G. K. Bakshi, "The weight distribution of some irreducible cyclic codes," *Finite Fields and Their Applications*, vol. 18, no. 1, pp. 144–159, 2012.
- [10] G. Vega, "The weight distribution of an extended class of reducible cyclic codes," *IEEE Transactions on Information Theory*, vol. 58, no. 7, pp. 4862–4869, July 2012.
- [11] B. Wang, C. Tang, Y. Qi, Y. Yang, and M. Xu, "The weight distributions of cyclic codes and elliptic curves," *IEEE Transactions on Information Theory*, vol. 58, no. 12, pp. 7253–7259, 2012.
- [12] J. Yuan, C. Carlet, and C. Ding, "The weight distribution of a class of linear codes from perfect nonlinear functions," *IEEE Transactions on Information Theory*, vol. 52, no. 2, pp. 712–717, 2006.
- [13] D. Zheng, X. Wang, X. Zeng, and L. Hu, "The weight distribution of a family of p -ary cyclic codes," *Designs, Codes and Cryptography*, pp. 1–13, 2013.
- [14] I. F. Blake and K. Kith, "On the complete weight enumerator of Reed-Solomon codes," *SIAM J. Discret. Math.*, vol. 4, no. 2, pp. 164–171, Mar. 1991.
- [15] K. Kith, "Complete weight enumeration of Reed-Solomon codes," *Master's thesis, Department of Electrical and Computing Engineering, University of Waterloo, Waterloo, Ontario, Canada*, 1989.
- [16] T. Helleseht and A. Kholosha, "Monomial and quadratic bent functions over the finite fields of odd characteristic," *IEEE Transactions on Information Theory*, vol. 52, no. 5, pp. 2018–2032, 2006.
- [17] C. Ding, T. Helleseht, T. Klove, and X. Wang, "A generic construction of Cartesian authentication codes," *IEEE Transactions on Information Theory*, vol. 53, no. 6, pp. 2229–2235, 2007.
- [18] C. Ding and X. Wang, "A coding theory construction of new systematic authentication codes," *Theoretical computer science*, vol. 330, no. 1, pp. 81–99, 2005.
- [19] W. Chu, C. J. Colbourn, and P. Dukes, "On constant composition codes," *Discrete Applied Mathematics*, vol. 154, no. 6, pp. 912–929, 2006.
- [20] C. Ding, "Optimal constant composition codes from zero-difference balanced functions," *IEEE Transactions on Information Theory*, vol. 54, no. 12, pp. 5766–5770, 2008.
- [21] C. Ding and J. Yin, "A construction of optimal constant composition codes," *Designs, Codes and Cryptography*, vol. 40, no. 2, pp. 157–165, 2006.
- [22] A. Kuzmin and A. Nechaev, "Complete weight enumerators of generalized Kerdock code and linear recursive codes over Galois ring," in *Workshop on coding and cryptography*, 1999, pp. 333–336.
- [23] —, "Complete weight enumerators of generalized Kerdock code and related linear codes over Galois ring," *Discrete applied mathematics*, vol. 111, no. 1, pp. 117–137, 2001.
- [24] C. Li, Q. Yue, and F.-W. Fu, "Complete weight enumerators of some cyclic codes," *Designs, Codes and Cryptography*, pp. 1–21, 2015.
- [25] K. Ding and C. Ding, "Binary linear codes with three weights," *IEEE Communications Letters*, vol. 18, no. 11, pp. 1879–1882, Nov 2014.
- [26] C. Ding, "Linear codes from some 2-designs," *IEEE Transactions on Information Theory*, vol. 61, no. 6, pp. 3265–3275, June 2015.

- [27] K. Ding and C. Ding, "A class of two-weight and three-weight codes and their applications in secret sharing," *arxiv:1503.06512v1*.
- [28] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," *DSN progress report*, vol. 42, no. 44, pp. 114–116, 1978.
- [29] C. Carlet, C. Ding, and J. Yuan, "Linear codes from perfect nonlinear mappings and their secret sharing schemes," *IEEE Transactions on Information Theory*, vol. 51, no. 6, pp. 2089–2102, 2005.
- [30] R. Lidl and H. Niederreiter, "Finite fields," *Encyclopedia of Mathematics and its Applications. Reading, Massachusetts, USA: Addison-Wesley*, vol. 20, 1983.